RFID - Tp1

Rappel Objectif

L'objectif de ce tp était de prendre en main le matériel RFID et de réaliser un programme permettant de lire les tags RFID et d'écrire des données sur les tags.

Mise en place

1. Première étape :

Installation des drivers pour le lecteur RFID

Lien : https://www.acs.com.hk/en/products/3/acr122u-usb-nfc-reader/

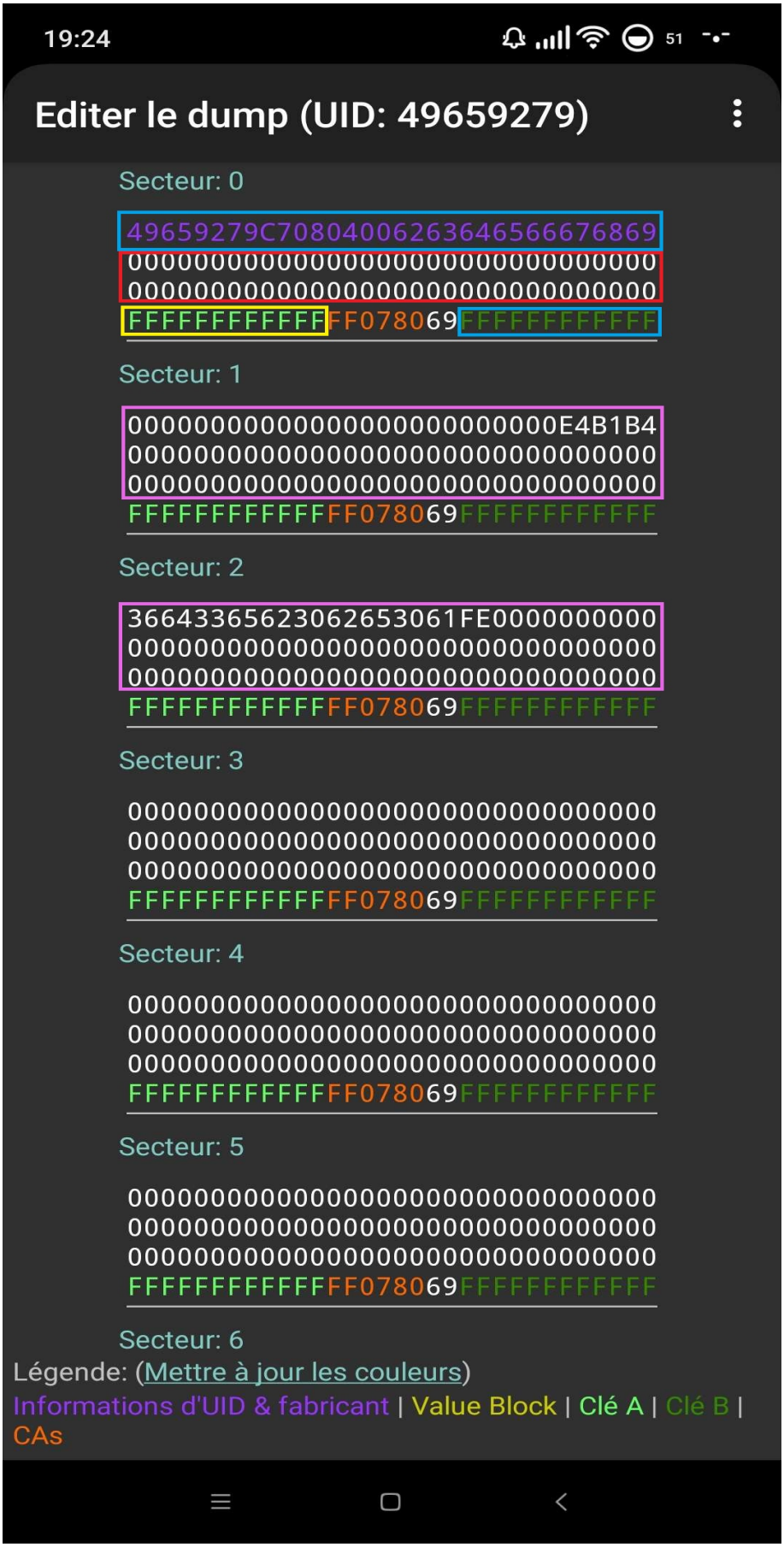
2. Seconde étape :

Prendre en main la lib PCSC et comprendre le code fourni

3. Troisième étape :

Un tag RFID est découpé en secteur qui eux mêmes sont découpés en bloc.
Sur nos tag, nous avions 64 secteurs qui sont composés eux même de 4 bloc de 16 Octets hexadécimaux. \

Voici un screenshot de dump de tag :



Secteur 0 : La première ligne du secteur 0 contient le numéro de série du tag.

Ensuite, ce secteur est composé de deux blocs de 16 octets hexadécimaux réservés pour les données.

Le dernier bloc du secteur 0 est réservé aux clés de sécurité. Ce bloc contient deux clés de 6 octets chacune : **la clé A** et **la clé B**. Ces clés sont utilisées pour des raisons de sécurité. Elles permettent de contrôler l'accès en lecture et en écriture aux différents blocs de données du secteur, garantissant ainsi la protection des informations stockées contre les accès non autorisés.

Pour chaque secteur (FOR SECTOR_INDEX IN SECTORS) : Chaque secteur (SECTOR_INDEX) est structuré de la manière suivante :

Les trois premiers blocs de 16 octets hexadécimaux sont réservés pour le stockage des données. Le dernier bloc du secteur est, comme dans le secteur 0, dédié aux clés de sécurité. Il contient également deux clés de 6 octets : la clé A et la clé B.

On peut écrire sur n'importe quel bloc si et seulement si le matériel nous y permet. En effet, certains tag ne nous le permettent pas.

Partie Sécurité

La sécurité RFID ne peut pas se faire "complètement". C'est à dire qu'un tag RFID va utiliser des ondes et ne peuvent pas 100% être sécurisées et une personne malveillante peut répliquer à l'aide d'un flipper zéro le signal.
Certaines techniques peuvent être mises en place comme l'analyse comportemental ou bien la norme OCSP(Online Certificate Status Protocol). Il peut être intéressant également de mettre du rolling code. C'est à dire avec une clé échangée entre le tag et le support de scan et si l'écart est trop grand, le tag est refusé.
Donc grosso modo, le tag est juste une porte grande ouverte aux attaques et c'est ceux qui gravitent autours qui doivent être protégés contre différentes attaques physique et logiciel. Par ailleurs, on peut utiliser des étuits pour empêcher le clonage de la carte MAIS il suffit qu'un skimmer soit présent et on en revient au même problème. MAIS ça limite les possibilités de clonages.

Chiffrement ?!

- Par nature, un tag RFID / NFC est clonable et accessible par tous vu qu'il émet des ondes. En effet, rien ne peut contenir des ondes (hormis une cage de Faraday).
- On peut aussi se poser la question du chiffrement avec un tag. En effet, comme nous avons dit juste avant, par nature il est clonable donc même si on applique tout le chiffrement que l'on souhaite, le chiffrement ne sert. Il faut donc avoir de la donnée rotative à chaque fois que l'on badge le tag.
- Pour parler des données rotative on peut parler de rolling code.
  TLDR : Le rolling code permet d'avoir une valeur qui s'échange entre le tag et le scanner et qui va être modifier. On aura une plage d'autorisation et SI notre valeur sur le tag est en dehors du champ autorisé, on refuse le tag.
- Et pour finir, on peut faire de l'analyse comportementale. Par exemple, je ne peux pas badger à l'étage 7 et 10 secondes après à l'étage 1. C'est physiquement impossible.

  Voici une petite vidéo concernant le flipper zéro et les attaques rolling code et replay

Chose marrante à faire

On a parlé de clonage, si vous avez une WII et des Skylanders, tentez de les cloner avec un capteur RFID (votre téléphone peut fonctionner). Vous constaterez que c'est *open bar*. (Pourquoi pas ne pas récupérer les figurines skylanders et tester des choses...)